

This is the Expert Report on the “Font Insurance Case”. It is an overall review of the case facts and materials.

AGCS MARINE INSURANCE COMPANY,

Plaintiff,

v.

FONT INSURANCE, INC.; MANUEL J.
FONT-ORONÓZ, JANE DOE AND THE
CONJUGAL PARTNERSHIP FORMED BY THEM;
ABC INSURANCE COMPANY; and
DEFENDANTS
A AND B.

Defendants.

Expert Report on Font Insurance’s Responses

Overall Analysis

Thomas A. Leghorn

July 14, 2020

Table of Contents

Summary of Case Facts and Materials AGCS vs. Font Insurance 2

Documents Reviewed 3

Expert Response Documents 3

Part 1 – Detailed Analysis and Opinion of Questions and Interrogatories 4

NIST (National Institute of Standards and Technology) Cyber Security Framework 6

Cyber Security Non-Compliance 6

Items Requested for Production 7

Example of Network Commands to Execute - For Finding IP addresses 9

Common Network Commands..... 10

E-mail Address Book Example..... 11

Corporate E-Mail Identification 12

What Cyber Security Items Should Have Been Produced by the Defendant..... 13

 Router Logs Example..... 14

 Firewall Logs and Settings..... 15

 Router User Logs..... 15

 Router Security Logs 16

Vulnerability Standard Assessments..... 17

 Network Vulnerability Analysis Results 17

 Phishing E-Mail Example for a Financial Institution..... 18

 Excerpt of the Complaint Identifying the Phishing E-Mail Incident..... 19

Conclusion..... 20

Information Event Logs 21

Error Event Logs 22

FTC (Federal Trade Commission) Data Breach Policies..... 23

Summary of Case Facts and Materials AGCS vs. Font Insurance

During the course of this litigation, I was provided various documents for my review based on the legal matter at hand. Those documents which were provided by AGCS (Plaintiff) are listed below (In the Section listed “Documents Reviewed”). Based on the documents and responses from Font Insurance (Defendant), I am able to identify some key observations and opinions that are in support of the litigation and highlight critical areas of concern when considering a Cyber Security Program or even when referencing Computer Infrastructure Security Best Practices. The preliminary observations and opinions are listed in the documents provided in the section (“Expert Response Documents”).

If we consider the appropriate methods of securing computer and networking infrastructure to minimize risk of loss or damage, one must determine if the proper procedures and methods were instituted by Font Insurance for a Cyber Security Program. Identifying adherence to the “Best Practices Approach” or non-adherence to the Best Practices Approach can be shown by the Defendants’ responses to interrogatories. They are *(referenced in item 2, in the section of this report labeled “Documents Reviewed” - “First Set of Interrogatories*

11-19” as well as item 3 in “Documents Reviewed” - “Request for Production of Documents 11-19”). The responses by the Defendant appear to follow a pattern in all of the documents provided and listed in the section below titled “Documents Reviewed”. This pattern of response from the Defendant seems to be focused on avoiding or answering any relevant questions or providing any useful information. This prevents us from ascertaining the appropriateness of the defendant’s actions in instituting a proper Cyber Security Program to limit the risk of loss to themselves, their clients, their partners and more specifically to AGCS the (Plaintiff).

The remainder of this report will identify and provide a detailed analysis of the breakdown of questions and interrogatories presented to the Defendant. It will also show the obvious aversion the Defendant has to simply providing the requested content in the form of reasonable responses as would be expected by an organization that was following Cyber Security Best Practice for reducing the risk of loss or harm to all parties involved.

This report will also explain in detail how a Cyber Term like “Phishing Attack” was the result of Instructions being changed on an e-mail, which led to funds being sent to an unintended recipient. This can be understood more completely if we understand the definition of a “Phishing Attack”. Below is that Definition.

The Phishing definition is as follows - Phishing is a Cyber Attack that uses disguised emails as a weapon to cause harm or to benefit the perpetrator. The goal is to trick the email recipient into believing that the message is authentic and that it is providing details on something they want or need — a request from their bank, for instance, or a note from someone in their company or from one of their customers. The perpetrator’s go to great lengths to impersonate the actual individual’s e-mail account to elicit an outcome for their benefit at the expense of the unsuspecting individual that falls prey to their efforts.

These are also unscrupulous characters trying accomplish some type of nefarious gain. This is all at the expense of the unsuspecting individual. Sometimes this action is to click a link or download an attachment.

Documents Reviewed

- 1) N1429065 – Compliant -(Jan. 2020)
- 2) First Set of Interrogatories 11-19 - (Jan. 2020)
- 3) Request for Production of Documents 11-19 - (Jan 2020)
- 4) Defendants' Answers to Plaintiff's First Set of Interrogatories Final (00722628xC536D) - (Jan 2020)
- 5) Responses and Objections to Plaintiff's RPDs (00725319xC536D) - (Jan 2020)
- 6) Exhibit 19 Print 1 Add'l Wire Info needed-Signed document 12-13-17 TMS assessment work signed (Bates 000322-000329) - (Jan 2020)
- 7) Exhibit 15 Print 1, LLC (Bates 000233-000246) - (Jan 2020)
- 8) Exhibit 16 FirstBank - Wire Instructions - Print 1 (Bates 000247) - (Jan 2020)
- 9) Exhibit 17 Exposiciones y Riesgos de Responsabilidad Ciber - (Jan 2020)
- 10) Exhibit 18 Print 1, LLC - Wire Transfer \$500K-FTR0016551 COMPLETED-Clm #80139197 (Bates 000311-000321) - (Jan 2020)
- 11) 2019-09-26-Indicial-disclosure-enumerado – (Jan 2020)
- 12) Defendants' Answers to Plaintiff's First Set of Interrogatories Final (00722628xC536D)
- 13) Expert Disclosure of Mark Abramson February 10, 2020 (N1618084-1) - (Feb 2020)
- 14) C_Cajigas_CV_2019_06_23 (002) - (Feb 2020)
- 15) Responses and Objections to AGCS's Second Set of RPD (00741817xC536D) (002) - (Mar 2020)
- 16) NIST Security Best Practices – (Mar 2020)
- 17) 2020 05 01- Font's response to AGCS's Discovery Objection Letter (00749902xC536D) (003) – (May)

Expert Response Documents

- 1) CV/Resume and Background – (Feb 2020)
- 2) Information Security Perspective on Font Insurance – (Mar 2020)
- 3) cybersecurity-framework-021214 – (Mar 2020)
- 4) Opinion_On_Response_To_May_01_2020_Font_Insurance_Letter – (May 2020)
- 5) pdf-0154_data-breach-response-guide-for-business-042519-508 – (May 2020)

Part 1 – Detailed Analysis and Opinion of Questions and Interrogatories

After analyzing the document referenced above as *“RESPONSES AND OBJECTIONS TO PLAINTIFF’S FIRST REQUEST FOR PRODUCTION OF DOCUMENTS”* the following opinions and observations can be identified as stated below. Font Insurance (Defendant), has provided a response stating that the production requests and questions were overly broad and without merit. As a going concern, that deals with organizational data that is privileged and confidential a reasonable expectation of “Cybersecurity” (meaning and effort to implement programs that reduce the risk of loss or harm) should be implemented and adhered to by an organization that deals with financial data or any sensitive data on a regular basis.

If we examine the responses of the defendant closely, we see a pattern of non-responsive behavior and avoidance of providing information from requests that would seem reasonable to any other organization that had instituted proper Cyber Security and Infrastructure Security Controls.

To illustrate this point further, the general approach of an organization that deals with confidential client information, whether financial or personal, would normally be to follow the standards of Best Practice Cyber Security methods. This should be done to ensure the safety and integrity of their data and information as well as their clients. This is especially important in the case of electronic documents or e-mail. Much of the information done in business today is through email exchanges between various parties. That is why organizations such as NIST (*National Institute of Standards and Technology*) has developed and supported a program for Cyber Security, which includes the security of email systems such as what was used by the Defendant.

The NIST Framework shown below is a standard that most responsible organizations follow, when they are in the process of securing their technology infrastructure, such as their e-mail systems. Had the Defendant proceeded to follow these standards such as “Identify” the vulnerabilities in their computing and networking infrastructure, they would have been aware of potential areas of weakness or where possible breaches might occur that would allow perpetrators to penetrate the vulnerabilities of their email system. Once these vulnerabilities were identified, the appropriate action would be to follow Cyber Security Methods to “Protect” the computing and networking environment from risk or potential loss. Had the Defendant shown any effort to execute the protect phase, there would have been “Network Logs”, or “Event Logs”, or “Message Logs” indicating the series of events that led to the breach of the Defendant’s email system and the potential for a Phishing Attack. This Phishing Attack is

preventable or at the very least “Detectable” and trackable by the implementation of a Cyber Security Program.

This leads us to another phase of the NIST Process. “Detect” is an important part of a Cyber Security Program and it helps to stop the infiltration of unwanted Cyber Criminals as well as Phishing Scams that play on Security Weaknesses of an organization’s email system.

In **(Section III Specific Responses, Question 1) of Font Insurance’s Responses and Objections**, a specific request for any type of “logs” was issued to the Defendant to determine if the email breach was detectable by the Defendants Cyber Security Program. Based on the non-responsive nature of the Defendant, it appears as if they did not follow the NIST “Detect” process. Had the Defendant followed this approach in the NIST Program and Framework, they would have also been able to execute the next phase of the NIST Program called “Respond”. In **(Section III Specific Responses, Question 2) of Font Insurance’s Responses and Objections**, it was noted that the Defendant had networking equipment called a **Cradlepoint Router**. The Cradlepoint Router has a logging mechanism that allows for “detection” of many types of nefarious intruders to an organizations network. This is in line with the NIST approach for “detection” and also leads to the NIST Phase of “Respond”. The Defendant would have had the immediate ability to “Respond” to their email breach. The Defendant would have also detected that the email system was compromised based on the Phishing email that was used to perpetrate the fraudulent email that AGCS received, which included information requesting a change of “Financial Information”. Had the Defendant executed standard Cyber Security Operating Procedures under the NIST Framework, they would have been able to “Recover” all pertinent information from the Cradlepoint Router Logs, to assist in the recovery of the email vulnerabilities that provided the perpetrators a means of penetrating the Defendants email system and allowed them to impersonate the intended individual responsible for the email at Font Insurance.

NIST (National Institute of Standards and Technology) Cyber Security Framework

Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Again, referencing the NIST Framework above, had the defendant been able to provide “IP Address” Information as requested in **(Section III Specific Responses, Question 3) of Font Insurance’s Responses and Objections**, there would have been evidence of the Defendant’s effort around instituting some sort of Cyber Security Program to reduce the risk of loss to all parties involved. However, given the fact that the Defendant was unable to produce any such information, it stands to reason that the Defendant either had no knowledge of how to institute such a Cyber Security Program in its most rudimentary form or was negligent in not doing so.

Given these circumstances, it is not surprising that the Defendant continues to respond in the negative for each and every request in **(Section III Specific Responses, Questions 4 thru 14) of Font Insurance’s Responses and Objections**. This section highlights the need for following the NIST Framework. Had the Defendant conducted regular vulnerability assessments or some form of penetration testing, they would have had preventative measures in place to thwart email breaches that allow a large financial sum to be extracted by a nefarious perpetrator. The Defendant had no evidence of ever engaging in these preventative measures, given the fact they were unable to produce any document in the slightest form that represented a “Vulnerability Assessment” or and “Audit” of their Information Systems, including their email system. The Defendant’s actions show they exhibited no thoughtful or planned process to address any of the commonly requested information in their negative responses. Therefore, we can clearly see the defendant does not meet any recommended Information Security Standards or Processes and was unprepared for the events that followed and led to the breach of their email system by a Phishing Attack.

Cyber Security Non-Compliance

After review of “Font Insurance’s Responses and Objections to AGCS's Second Set of RPD”, as well as the “Discovery Objection Letter”, there is a good indication that Font Insurance (the Defendant), was not willing or able to provide the necessary responses to their Cyber Security Program or the lack of a Cyber Security Program.

If we review the details of the “Responses and Objections of Font Insurance” and the “Discovery Objection Letter” (Item15 and Item17, listed above, in the “Documents Reviewed” section of this document), we see that for each and every request under section “III. Specific Responses” of this document, the Defendant was unable to fulfill the request and appears to be non-responsive.

The requests for production of the following items are very appropriate and expected, when the objective is to understand what precautions the Defendant had in place to reduce the risk of a security breach or Cyber Crime attack or even a Phishing Attack on their e-mail system.

Items Requested for Production

The items requested for production were as follows;

- a) Business e-mail accounts
- b) Event logs
- c) Error logs
- d) Message logs
- e) Cradlepoint Router Logs
- f) Network Security Architecture
- g) Listing of all network hosts and domain servers and the IP addresses
- h) E-mail address or email account on the Microsoft E-mail System
- i) Microsoft Exchange Advanced Threat Protection Event Logs
- j) Windows Defender Antivirus Event and Message Logs,” including any Internal Log files from December 1, 2017 to January 31, 2018
- k) A copy of Font Insurance’s Antivirus Event and Message Logs from December 1, 2017 to January 31, 2018
- l) A copy of the Font Insurance’s Firewall Event Logs and Message Logs from December 1, 2017 to January 31, 2018.
- m) A copy of any Vulnerability Assessment Reports Font Insurance done internally or by any third party
- n) A copy of any Penetration Testing Assessment Reports Font Insurance Company has done internally or by any third part
- o) SIEM (Security and Information Event Management System), from December 1, 2017 to January 31, 2018

- p) A copy of any I.T. (Information Technology) Internal Audit Report performed on Font Insurance's network, Networking System and/or E-mail Platform
- q) A copy of any "Simulated Phishing Attack Tests" performed by Font Insurance or any third-party vendor
- r) A copy of any "Phishing E-mails" Font Insurance received between January 1, 2017 and January 31, 2018

All of the items requested above, (a thru r) are reasonable for understanding what the defendant had in place to protect the information and assets of Font Insurance (the Defendant). Each item listed above has a purpose in helping us to understand what condition the Defendant's Cyber Security Program is in and whether or not it was capable of managing threat situations or even had the ability to detect breaches of Information Security. From the request for emails (referenced item a above) to the request for various logs (referenced in items **b,c,d** and **e** above), there was a consistent non-responsive answer by the defendant for each and every request. These items are common items you would find in an I.T. department for Asset Control and Information Security Management.

Additionally, it would be expected that the Defendant's Information Security/ I.T. Specialist (**Mr. Rene Saez**), would have full knowledge and access to the "Network Security Architecture" documents of "Font Insurance". As part of a security breach mitigation strategy, it would be expected that the I.T. Specialist had procedures in place to thwart any potential Information Security Risks. The request for Production of (item **f** above "Network Security Architecture"), would be expected as a reasonable request for understanding the extent of the Defendant's Cyber Security Program. However, the Defendant's I.T. Specialist was unable to produce this information. Additionally, the Defendant was unable to comply with the request to produce (item **g** "*all network hosts and domain servers and the IP addresses*" shown above). As part of the Information Security Best Practices and outlined in documents such as the one "NIST" (National Institute of Standards and Technology) provides, it would be expected that the Defendant had a complete list of their computing and networking assets for tracking and managing.

Additionally, the Defendant could have fulfilled this request by executing standard "Networking" commands that are very basic knowledge that even a novice I.T. Specialist would be expected to know. An example of the commands for generating Networking Information on a particular computer system, either laptop or desktop are shown below.

Example of Network Commands to Execute - For Finding IP addresses

1. *ipconfig*

This command displays all network settings assigned to one or all adapters in the computer. You can find information such as your own IP, subnet, and Gateway.

2. *arp -a*

When you issue the “arp -a”, you’ll get IP-address-to-mac conversion and the allocation type (whether dynamic or static) of all devices in your network.

3. *Ping*

It helps determine connectivity between two hosts and find the IP address of a hostname.

a. Output of “ipconfig”

```
C:\ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : ircthailand.org

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : home
    Link-local IPv6 Address . . . . . : fe80::b551:2811:2df8:5208%11
    IPv4 Address. . . . . : 255.255.255.0
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 255.255.255.0

Tunnel adapter isatap.ircthailand.org:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Tunnel adapter isatap.home:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : home
```

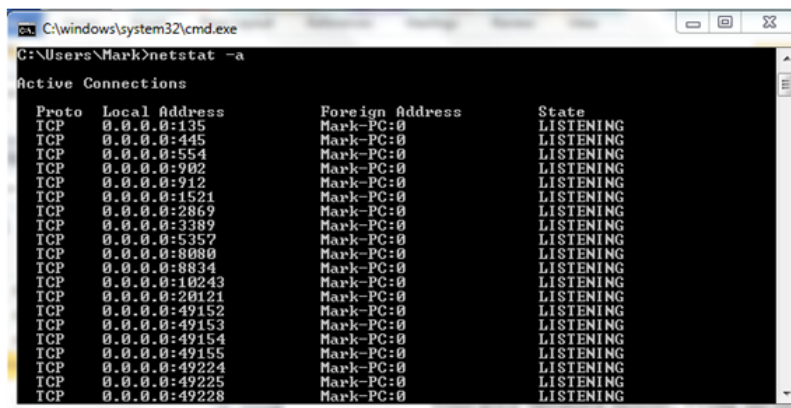
The above “ipconfig” command allows us to see the “Network IP Addresses” and to simply output the results to the screen. This is not overly burdensome for any somewhat skilled I.T. Professional.

Common Network Commands

Example: Of the Netstat – a command at a DOS command prompt.

(Note: The output of this information can be directed to a file by simply typing the following command at the DOS command prompt.)

```
C:\Users\Mark> netstat -a > c:\MyDocuments\Netstat_OutPut_File.TXT
```



```

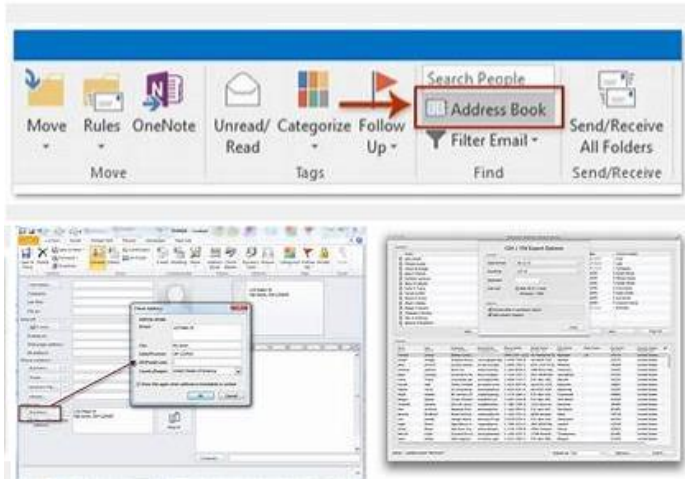
C:\Users\Mark>netstat -a
Active Connections
Proto Local Address           Foreign Address         State
TCP    0.0.0.0:135              Mark-PC:0               LISTENING
TCP    0.0.0.0:445              Mark-PC:0               LISTENING
TCP    0.0.0.0:554              Mark-PC:0               LISTENING
TCP    0.0.0.0:902              Mark-PC:0               LISTENING
TCP    0.0.0.0:912              Mark-PC:0               LISTENING
TCP    0.0.0.0:1521             Mark-PC:0               LISTENING
TCP    0.0.0.0:2869             Mark-PC:0               LISTENING
TCP    0.0.0.0:3389             Mark-PC:0               LISTENING
TCP    0.0.0.0:5357             Mark-PC:0               LISTENING
TCP    0.0.0.0:8080             Mark-PC:0               LISTENING
TCP    0.0.0.0:8834             Mark-PC:0               LISTENING
TCP    0.0.0.0:10243            Mark-PC:0               LISTENING
TCP    0.0.0.0:20121            Mark-PC:0               LISTENING
TCP    0.0.0.0:49152            Mark-PC:0               LISTENING
TCP    0.0.0.0:49153            Mark-PC:0               LISTENING
TCP    0.0.0.0:49154            Mark-PC:0               LISTENING
TCP    0.0.0.0:49155            Mark-PC:0               LISTENING
TCP    0.0.0.0:49224            Mark-PC:0               LISTENING
TCP    0.0.0.0:49225            Mark-PC:0               LISTENING
TCP    0.0.0.0:49228            Mark-PC:0               LISTENING

```

Using the “ipconfig” or “netstat” commands on the computer systems on the Font Insurance Network would have been one possible way for the Defendant to comply with the production request of AGCS for IP Address Information and Networking Information such as port addresses.

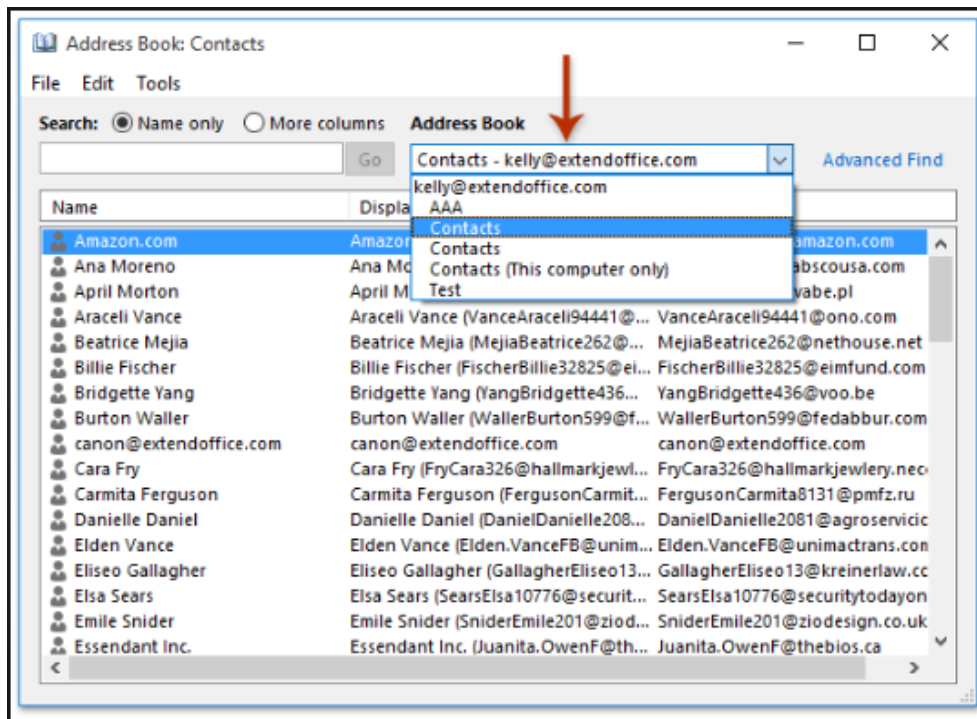
If we look at (item **h** “E-mail address or email account on the Microsoft E-mail System” above), the request for this information is completely expected and certainly, would not seem overly burdensome, given the fact that Font Insurance uses e-mail to communicate regularly with its business partners such as AGCS. Most any user today that is on a computer system has access to an e-mail account, especially, when the e-mail account is in a corporate setting. At a minimum, the Defendant would have the ability to create screen shots of the corporate e-mail accounts such as the screen shot example shown below.

E-mail Address Book Example



In the example screen shot above, it shows what a Microsoft Outlook Mailbox Address book would look like had the Defendant provided a list of their e-mail accounts. This is an indication of how easy it would have been for the Defendant to comply with the request in (item **h** “*E-mail address or email account on the Microsoft E-mail System*” above). A further detailed view of the E-mail Address Book is shown below.

Corporate E-Mail Identification



This is an illustration of how easy it is to create a corporate E-Mail Address Book and how easy it would have been for the Defendant to comply with the request for production as stated by AGCS. This simple screen shot contains the listing of E-mail Addresses and would have provided some insight into the accounts that were on the Font Insurance E-Mail System. This is important because E-Mail Systems must be secured as part of a Cyber Security Program to reduce the possible risk of breach or intrusion. If the Defendant is being diligent in keeping up with their Information Security Best Practices or even minimal practices of securing Font Insurance's corporate network, they would have been able to produce a "Corporate E-Mail List" as requested in (item **h** mentioned above).

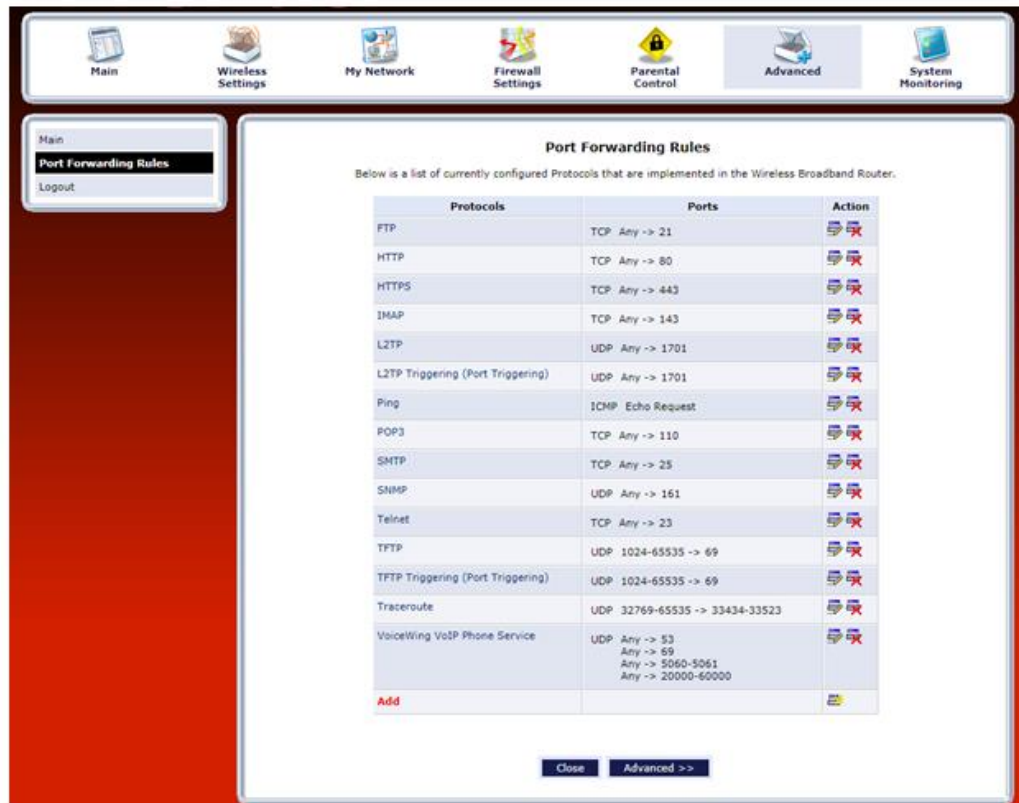
In (items **i, j, k** and **l** shown above) the request for production is expected and necessary for understanding the ability of Font Insurance to track normal networking, computing systems and , e-mail activity on their own Corporate Infrastructure. The (Event Logs, Error Logs, Message Logs and Firewall Logs) of a Corporation are vital assets that should be monitored and readily available for any I.T. Specialist to view at a moment's notice. This ability to produce and examine them is part of a well equipment Information Security Program. It is also part of a Best Practices Approach for reducing the risk of breaches or risk of loss of an organization's confidential assets like what happened at Font Insurance.

What Cyber Security Items Should Have Been Produced by the Defendant

Font Insurance was unable to produce any log information in the request for production based on (items **I, J, K** and **L**). This seems completely unusual because this is a basic request, that almost any Information Security Professional would understand and have the ability to produce. There are standard tools that are available to even the most novice I.T. Specialist for extracting “log” information. This information would assist in this request and would eliminate the need for being non-responsive.

If we consider that Font Insurance had a “Cradlepoint Router”, then it stands to reason that they had the ability to produce “Router Logs” that would assist everyone. This includes Font Insurance and would help with the understanding of what type of vulnerability might have existed in their Computer Network or Infrastructure. Below is an example of what accessing a “Router” such as the “Cradlepoint Router” that Font Insurance used in its Networking Environment, would look like.

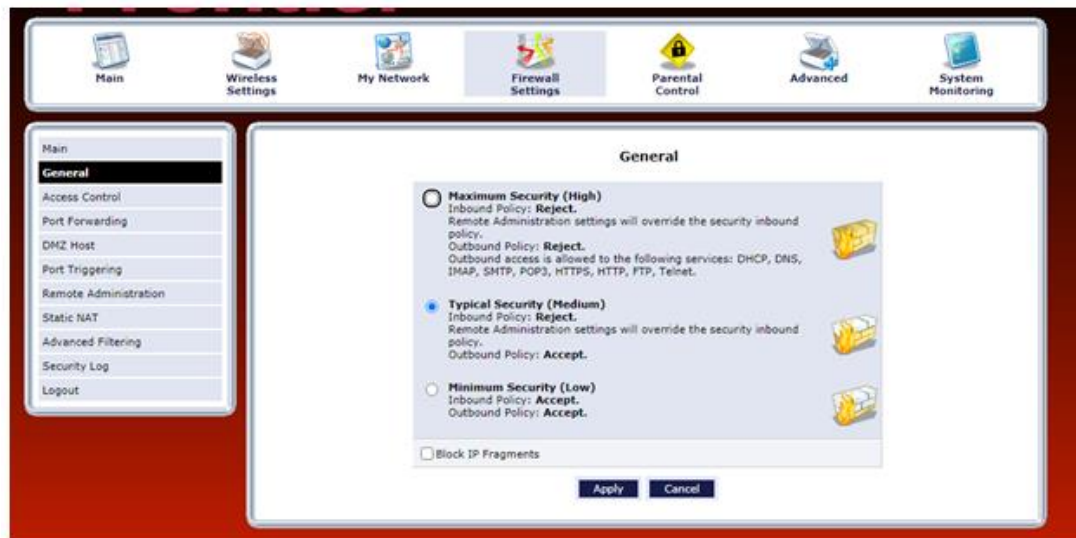
Router Logs Example



If we notice in this example "Router Administration Screen", there is a listing of what is called "Networking" Ports. This is an "Entrance" and "Exit" point of a Company's "Networking" environment. If we had the "Cradlepoint" Router Logs, we would be able to detect if Font Insurance had unauthorized entry on their Computer Network through a potential vulnerable "Port Address" as is listed in the example screen shot above.

Additionally, the "Router" provides a means of monitoring what is called a "Firewall". The Firewall is also accessible via the "Router's Administration" screen and would look like the screen shot below. The "Firewall" settings indicate how access is set up for Internal Computer Network Users as well as External Network and Intranet Users. This would help lead us to whether Font Insurance had the appropriate settings on their "Firewall" to prevent intrusion. It would also indicate if Font Insurance was following a Best Practice Approach for setting up the Firewall.

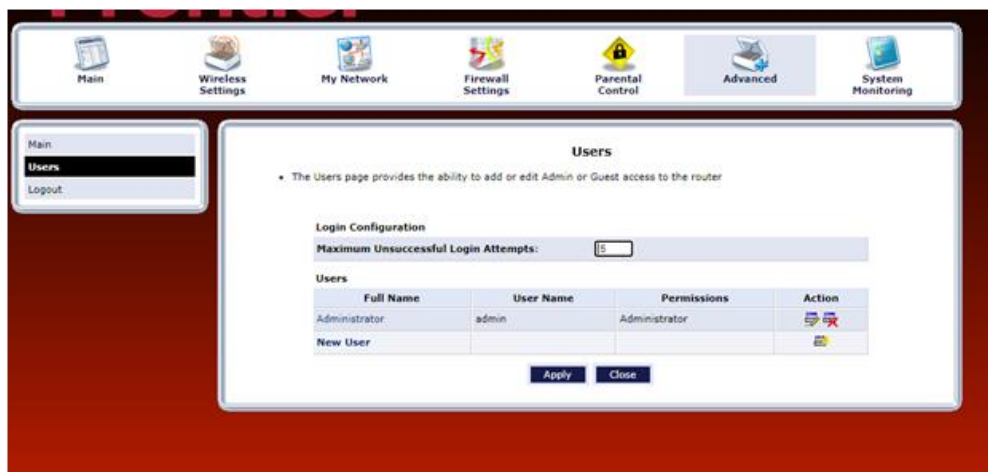
Firewall Logs and Settings



Given the screen shot above of the example “Firewall” settings, we can see that an I.T. Specialist with minimal effort would be able to access this information and therefore, be able to fulfill the production request as was shown in (item L above “Firewall Logs”).

Some of the additional settings of the “Router” would include access to the network users and would therefore, show authorized users as well as unauthorized users on Font Insurance’s Computer Systems or Networking Infrastructure. If we view another screen shot of an example “Router Log or Configuration”, we will see the ability to list users on the “Router Administration Page”.

Router User Logs



The “User Section” of the “Router Administration Page” provides an I.T. Specialist the ability to see the users on the network and to manage their access. As a matter of standard Information Systems Security Practices and as a Best Practice Approach, this information should be monitored and reviewed on a

regular basis. If Font Insurance was diligent in this practice, they would have had this information readily available to be produced in the request for production as stated in (item g “IP Addresses”, shown above).

Furthermore, “Routers”, such as the “Cradlepoint Router that is employed by Font Insurance as part of their Networking Infrastructure, have the ability to review “Security Logs” that indicate intrusion on the network and help to alert to unwanted access. As a standard practice, the I.T. Specialist would be expected to monitor and review these logs. Examples of the “Router Security Logs” are shown below in the screen shot.

Router Security Logs

The screenshot displays the Cradlepoint Router Administration Page. At the top, there is a navigation bar with icons for Main, Wireless Settings, My Network, Firewall Settings, Parental Control, Advanced, and System Monitoring. On the left side, there is a sidebar menu with options: Main, General, Access Control, Port Forwarding, DMZ Host, Port Triggering, Remote Administration, Static NAT, Advanced Filtering, **Security Log**, and Logout. The main content area is titled "Security Log" and contains a table of log entries. Above the table are buttons for Close, Clear Log, Save Log, Hazard, Settings, and Refresh. Below the buttons is a note: "Press the Refresh button to update the data."

Time	Event	Event-Type	Details
Jul 27 19:44:50 2020	Firewall Setup	Configuration change	WBM user Unknown (0.0.0.0) has changed security settings[repeated 3 times, last time on Jul 27 19:44:51 2020]
Jul 27 19:42:39 2020	Firewall Info	User authentication success	Username: admin from 192.168.1.16
Dec 14 19:00:19 2007	Firewall Setup	Configuration change	WBM user Unknown (0.0.0.0) has changed security settings[repeated 2134 times, last time on Jul 27 19:29:30 2020]
Dec 14 19:00:11 2007	Firewall Setup	Firewall status changed	enabled
Dec 14 19:00:10 2007	System Log	Message	The system is UPI

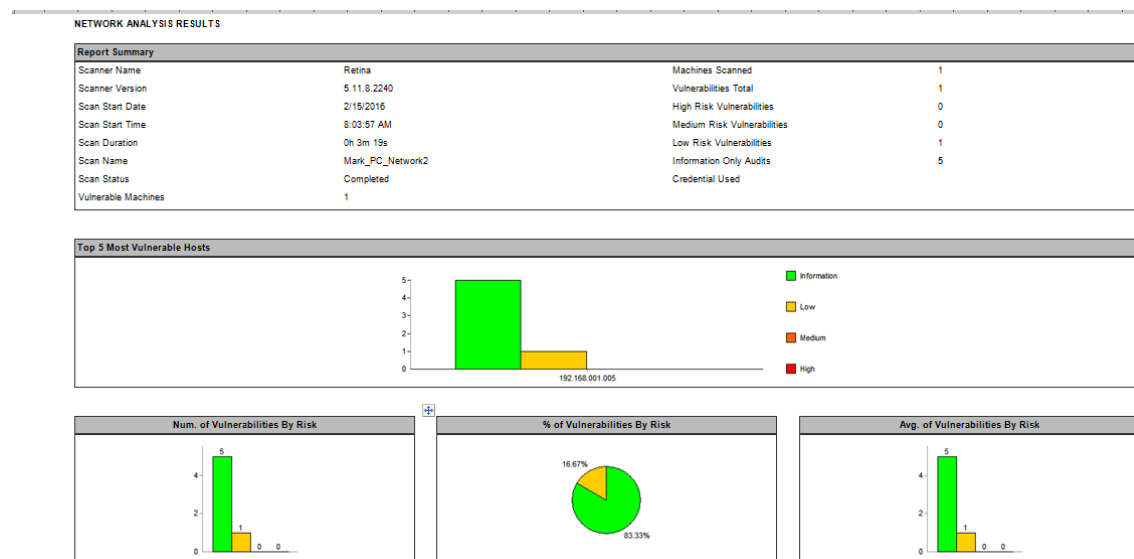
As can be seen in the example screen shot above, there is easy access to the “Firewall Logs” as well as the “System Logs” of the “Router” in one place. The I.T. Specialist for Font Insurance should have been able to fulfill the request for production with limited effort using the existing interface of the “Cradlepoint Router Administration Page”. It is not very burdensome to access readily available security information that should be monitored and viewed on a regular basis, if an organization is following “Cyber Security Best Practices”.

Vulnerability Standard Assessments

If we review request for production (item **m** “*Vulnerability Assessment Reports*”), we see that this is another means for maintaining a secure computing and networking environment, as Font Insurance should have been doing as part of their Cyber Security Protection Program. If Font Insurance was diligent in their efforts to maintain a standard of care for an appropriate Cyber Security Protection Program, they would have had regularly scheduled “Vulnerability Assessments”. The output of the Vulnerability Assessment would provide feedback to Font Insurance and their I.T. Specialist to manage any potential **Risks** or Loss of Information that could be incurred by Font Insurance if a breach occurred.

An example of a Vulnerability report might look like the screen shot below.

Network Vulnerability Analysis Results



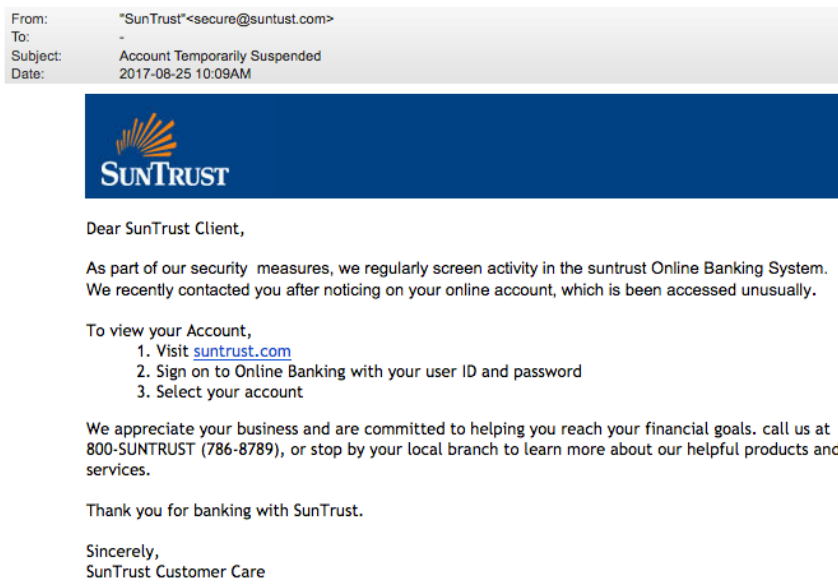
This example vulnerability report illustrates areas of a network that are tested and examined for potential issues that could lead to a breach or have some type of security risk. If Font Insurance engaged in normal Cyber Security Practices, we should fully expect that they would have some third party organization or even an internal effort to conduct some form of vulnerability assessment. Therefore, they would have been able to meet the request for production as stated in (item **m** “*Vulnerability Assessment*”, shown above). It was noted in (item **17** above “*2020 05 01- Font's response to AGCS's Discovery Objection Letter*”), that Font Insurance’s Law Firm engaged a Third Party Firm to conduct an assessment for them because of the breach. It would be expected that as part of the engagement, there would have been a report provided to Font Insurance on the Companies (*Florida Based Cyber Security Firm’s*) findings based on their assessment. As a matter of compliance and forthrightness, we would expect Font Insurance to provide the detail of this assessment as part of the request for production as it relates to (item **m** “*Vulnerability Assessment*”, shown above).

If we further consider the items listed above in (N, O, P, Q, and R), they represent a sound process for identifying, tracking, monitoring and responding to Information Security Protection Objectives. This can be found in the NIST Reference. These items involve executing Cyber Security tests for vulnerability. They include “a Penetration Test”, which would indicate any openings on the Font Insurance Network that could potentially let nefarious individuals on their network. They also include “E-Mail Phishing” tests that detect and alert individuals about fraudulent e-mails that could cause harm or damage to the business of Font Insurance as well as to its partners or clients. There are good reasons for these Cyber Security tests as we can see by the purported incident at Font Insurance that led to this litigation. Currently, Font Insurance has not provided any evidence of these types of Cyber Security and Vulnerability tests or documents showing they were performed. Had these items been provided, an assessment of Font Insurances preparedness for breaches or risk of loss could have been methodically analyzed and investigated.

One of the items mentioned above is a test for Phishing e-mails. This is something most organizations do today because it is becoming more and more prevalent in institutions dealing with financial transactions. Based on the details of this case, it appears that there was a “Phishing e-mail” attack on Font Insurance that was successful. Had Font Insurance been diligent in their Cyber Security Protection Program efforts, they would have done simulated Phishing e-mails to prepare their staff in the event that one occurred. They would have been better trained to anticipate and recognize suspicious e-mails. It appears that Font Insurance and its representatives were caught by a Phishing E-mail. This example below shows what a suspicious e-mail contains in a test environment and would most likely have prepared Font Insurance’s staff on how to handle it or at least give them a clue on what to be aware of in this situation.

Phishing E-Mail Example for a Financial Institution

Phishing email example: Account temporarily suspended



In the above example Phishing e-mail, there are clues on what to look for and how to address such an e-mail under training conditions. This would be executed as part of a Vulnerability Assessment. Had Font Insurance and its staff gone through this exercise, they may have prevented the successful execution of the Phishing E-mail attack.

One of the premises of this vulnerability testing is identifying suspicious types of e-mail communications. We have seen through the documents of this litigation that Font Insurance did have the opportunity to potentially stop the Phishing e-mail attack if their staff had recognized the content of the Phishing e-mail. The screen shot below shows the Complaint in this case, highlighting Font Insurance's failings to properly secure its computing and e-mail environment. Had they engaged in the proper procedures of a Cyber Security Program and instituted some form of Vulnerability Assessments on their E-Mail System, this Phishing Incident may have been prevented.

Excerpt of the Complaint Identifying the Phishing E-Mail Incident

42. Font Insurance and Font-Oronóz breached their duty and acted negligently in a variety of ways including, without limitation:

- a. by failing to act on December 15, 2017, when put on notice on at least two occasions that the wiring instructions for the partial settlement proceeds were fraudulently altered;
- b. by allowing a third-party to gain access to its e-mail account and wrongly issue wire instructions to AGCS which resulted in \$500,000 being wired to a party not entitled to receipt of the money;
- c. by using an unsecure, unencrypted e-mail account when communicating sensitive information for hundreds of thousands of dollars;
- d. by failing to ensure that the sensitive information was protected;
- e. by failing to ensure that AGCS was correctly apprised of where to wire the partial settlement proceeds at issue;
- f. by failing to identify the fraudulent activity that led to the loss; and,
- g. by failing to implement and maintain reasonable security measures and procedures to protect confidential and sensitive financial information from access or use by unauthorized people.

As shown above, the complaint excerpt highlights an essential premise of Phishing e-mails. That is, the perpetrator executes a fraudulent request and the unsuspecting party acts on it and therefore, incurs a loss due to the efforts of the perpetrator. This could have potentially been avoided if Font Insurance and its staff were equipped with knowledge that is gained from a vulnerability assessment. This would have been included in training on Phishing e-mails and how to identify them and react to them.

Finally, if we examine the approach that Font Insurance took to review the computer hard drive and have it reformatted, we see another misstep by Font Insurance in a Best Practice Approach of a Cyber Security Program. Font Insurance had an important piece of the breach erased, which to the novice computer user would appear to have removed the information permanently. This action was not in accordance with proper Cyber Security or Digital Forensics Procedures. The root cause of the breach can be traced by reviewing the hard drive where the incident occurred. Proper Cyber Security Procedures would dictate using a preservation approach on the hard drive to forensically review the hard drive for traces of tampering or intrusion. It would be expected that the “Third Party Florida based Cyber Security and Digital Forensics Firm” would have advised Font Insurance to Forensically Review the hard drive where the incident occurred. We would expect to see this recommendation in the results report had Font Insurance provided this report as part of the request for production.

Furthermore, through Forensic Techniques, it is possible to resurrect this information from the existing hard drive even after the drive is formatted. If Font Insurance had knowledge of the principles of Cyber Security Best Practices, they would also have known or been advised by their I.T. Specialist or Third Party Cyber Security and Digital Forensics Firm, that it is possible to still identify the root cause of the breach. This would be done by performing a Forensic Analysis on the Computer Equipment and Hard Drive that was involved in the Phishing Attack and System Breach. Additionally, if they had done what is called a “Clone”, Backup Copy, Disk Image or some preservation approach as prescribed by Cyber Security and Digital Forensics Best Practices, they would have been able to provide the requested information as stated in (item17 above “2020 05 01- Font's response to AGCS's Discovery Objection Letter (00749902xC536D) (003) – (May)”). In this “Discovery Objection Letter”, Font Insurance incorrectly states that the information could not be recovered. It can be recovered by Forensic Techniques and had Font Insurance followed Cyber Security and Digital Forensics Best Practices by using the proper “Chain of Custody Methods” used in a Digital Investigation, they would have a preserved copy of the hard drive of Mr. Font for further investigation and to meet the request for production.

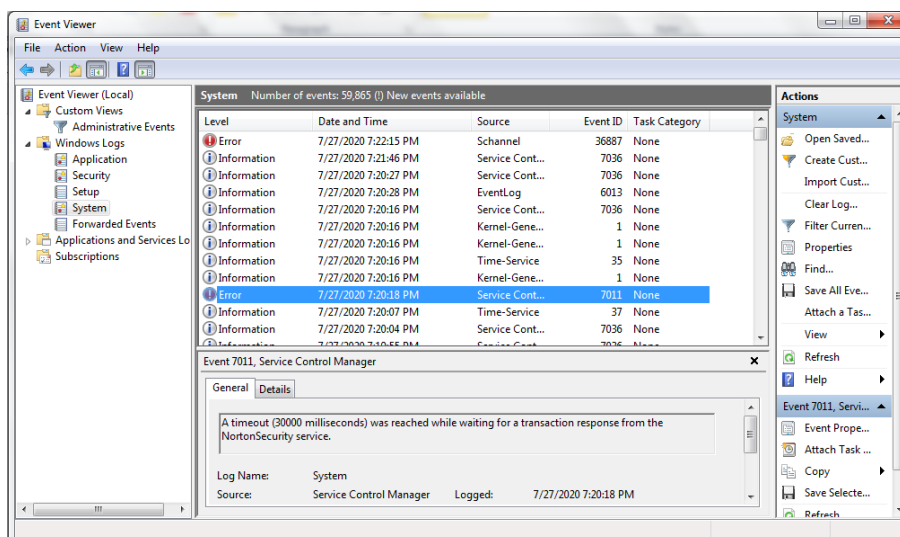
Conclusion

After careful consideration of the various items identified above in this document, we can clearly see that Font Insurance did not have adequate control of its Network, Computer Equipment, E-Mail System and Cyber Security Program. I have compared Font Insurance’s non-responsive answers with what is possible and what can be done by the most novice I.T. Specialist and there is a definite indication that Font Insurance is not being forthright with the items listed in each request for production. In the list above in the section “Items Requested For Production”, I have listed all of the items requested for production to help us understand the state of Font Insurance’s Cyber Security Program. This also indicates what their efforts included as part of an effort to reduce the risk of loss or damage to their own assets, computer and networking infrastructure as well as their partners and customers. Each item (a thru r) requests Cyber Security items that we would normally expect to see on a routine basis used and managed by Cyber Security Professionals as well as I.T. Specialists. Yet Font Insurance claims each item is non-existent or overly burdensome to provide for review and investigation.

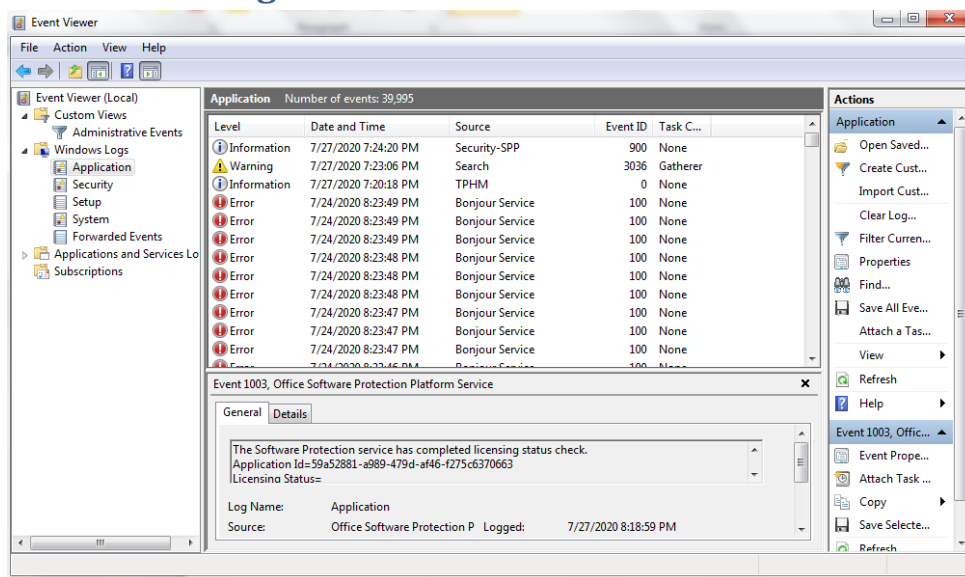
Whether we are speaking of a “Computer Network Architecture Diagram” or a “Listing of Network IP Addresses” or even an “Employee E-mail List”, each and every answer by Font Insurance is non-responsive or in the negative. If we review the NIST Guide on a Cyber Security Program, we can see that all of these items are standard items and part of a Cyber Security Best Practice Approach. Font Insurance did not engage with the core tenants of a Cyber Security Program such as “Identify”, “Protect”, “Detect”, “Respond” and “Recover”. This is completely evidenced by the fact that Font Insurance could not provide a single document to “Identify” any computer or networking assets being used in their organization. There was no evidence that Font Insurance was able to “Protect” their network, computers or e-mail system based on the lack of documentation provide in each request for production. There were no Cyber Security Measures in place to “Detect” the breach of their e-mail system by a Phishing Attack. As part of the (item **b**, *Event Logs*) request for production, which is listed in the section above titled (“*Items Requested for Production*”), we would have expected to see some type of analysis by Font Insurance on the “Event Logs”. This is on the top of the list of any “Detection” effort when investigating a security breach. Additionally, the event logs should be reviewed on a regular basis as part of a Cyber Security Best Practices Approach.

Had Font Insurance provided their “Event Logs”, they may have shown information as displayed in the screen shot below. These “Event Logs” as shown below, give insight into the activity on a particular computer and would be a good source for alerting an Information Security Professional or even an I.T. Specialist on areas of Security Risk or potential unwanted intrusion or activity that could lead to a breach such as a Phishing e-mail attack.

Information Event Logs



Error Event Logs



Another important point to recognize is that the Windows Event logs (both “Information” and “Error” type as shown above) have different purposes and display messages indicating activity on a particular computer system. The level of message indicates a minor or major activity and therefore, provides the Security Professional or I.T. Specialist an alerting level to “Respond” appropriately. This is one of the tenants of the Cyber Security Program. To “Respond” appropriately based on whether the “Event Log” has a “Warning” or “Critical” message. Currently, it is unknown if Font Insurance had any advanced notice of the breach that occurred on their e-mail system. If they were able to provide the “Event Logs”, this information is more likely to be ascertained. Given the fact that Font Insurance was unable or unwilling to provide their “Event Logs”, it has to be assumed they did not follow the appropriate Cyber Security Best practices for capturing this “Event Log” Information.

As part of an appropriately executed Cyber Security Program, the last action to consider, from a best practices approach, would be to understand how to recover from a Security Breach, Intrusion or Cyber Attack. The methods prescribed in the NIST Model indicate that the scene of the event or environment should be preserved for a “Root Cause Analysis”. This is a method for determining what happened during the breach and how to uncover the root cause of it and prevent future incidents from reoccurring.

It can clearly be shown that Font Insurance and its I.T. Specialist and Consultants, were not following this Cyber Security Best Practice approach, when they reformatted Mr. Font’s computer hard drive. The appropriate method would have been to preserve the information on Mr. Font’s hard drive before taking any action to remove a potential issue. Furthermore, Font Insurance was unable to provide any “Virus Logs or Malware Logs” that indicated they had a virus that potentially allowed for the e-mail Phishing Attack and Security Breach. Font Insurance indicates in “**Response to Supplemental Request Nos. 1 and 2:**” that there was a possibility of a virus that caused the e-mail Phishing Attack. However, they had no substantial “Virus or Malware Logs” that indicated such an event occurred.

As part of an expected Cyber Security Best Practice, Font Insurance should have routinely been monitoring these “Virus and Malware Logs” and had immediate access to them, which should not have been overly burdensome.

Throughout this report the theme has been the same. AGCS has requested in good faith the most common Cyber Security Artifacts, such as E-mail Lists, Network Architecture Diagrams, IP Addresses, Log files and Certified Reports indicating that Font Insurance had some type of Cyber Security Program in Place. Given all of the analysis and facts provided in this report, currently, there is no evidence that Font Insurance took the appropriate precautions to reduce the risk of loss to themselves and their business partners.

Additionally, under Cyber Security Best Practices and Even Stated in the “FTC’s Data Breach Policies”, Font Insurance should have followed proper protocol by addressing their e-mail system breach and alerting all appropriate parties as well as taking the appropriate action to reduce the risk of further loss. Below is a statement supporting this issue of non-compliance with support from the FTC Policies Guide.

FTC (Federal Trade Commission) Data Breach Policies

Under current widely accepted Federal and Local policies (FTC Policies), data breaches should be made known to the public as a matter of being forthright and good practice. The FTC Policies document on “Data Breach Response” outlines some best practice approaches on what should be done if a suspected breach or actual breach occurs. Below is a screen shot for convenience purposes of the basic approach that should be taken to “Secure Your Operations”, which Font Insurance appeared to completely ignore or was not aware of as a responsible organization.

DATA BREACH RESPONSE

A Guide for Business




Federal Trade Commission | business.ftc.gov

Secure Your Operations

Move quickly to secure your systems and fix vulnerabilities that may have caused the breach. The only thing worse than a data breach is multiple data breaches. Take steps so it doesn't happen again.

Mobilize your breach response team right away to prevent additional data loss. The exact steps to take depend on the nature of the breach and the structure of your business.

Assemble a team of experts to conduct a comprehensive breach response. Depending on the size and nature of your company, they may include forensics, legal, information security, information technology, operations, human resources, communications, investor relations, and management.

- **Identify a data forensics team.** Consider hiring independent forensic investigators to help you determine the source and scope of the breach. They will capture forensic images of affected systems, collect and analyze evidence, and outline remediation steps.
- **Consult with legal counsel.** Talk to your legal counsel. Then, you may consider hiring outside legal counsel with privacy and data security expertise. They can advise you on federal and state laws that may be implicated by a breach.

Secure physical areas potentially related to the breach. Lock them and change access codes, if needed. Ask your forensics experts and law enforcement when it is reasonable to resume regular operations.

In conclusion, it should be understood, that this report has completely identified what was lacking on the part of Font Insurance's Cyber Security Program as well as their non-responsive answers for request for production of the most basic Cyber Security Artifacts.

They even tried to invoke the Federal Rules of Civil Procedure in regards to Rule 26 on e-Discovery as a means to avoid providing basic information that is not overly burdensome and can be readily provided, which was clearly identified throughout this report. The examples shown above in this report illustrate this completely. Therefore, requesting standard Cyber Security documents and files is not overly burdensome for a properly maintained computing environment or even a minimally instituted Cyber Security Program, which Font Insurance seems to have none. The responses are not in the spirit of being forthright and are indicative of the inability to cooperate or a complete lack of knowledge in the area of Information Technology and Cyber Security as a whole.

Given the facts in this case and the complete details I have outlined in this report, it is abundantly obvious that Font Insurance did not have the appropriate controls in place, nor did they have even the most basic Cyber Security Program in place to prevent the actions caused by the Phishing e-mail. Those actions were what allowed a Phishing e-mail to be accepted as an authentic request for transferring a large sum of money to a nefarious recipient instead of the actual intended party. Furthermore, had Font Insurance had an appropriate Cyber Security Program in place, this legal matter may have been avoided.